NC STATE UNIVERSITY

CSC 495.002 – Lecture 1
Course Introduction

Dr. Özgür Kafalı

North Carolina State University
Department of Computer Science

Fall 2017

Basics

- Dr. Oz
- Email: rkafali@ncsu.edu
- Moodle for announcements and assignments
- Course website: https://ozgurkafali.github.io/courses/ncsu/csc495
- Hours: MW 11:45AM-1:00PM
- Location: EB2 1226
- No TA

Grading

- 30% – Individual homework assignments (4 best grades out of 5 assignments)
- 30% – Two group case studies (analysis and in class presentation)
- 40% – One group project (project report and in class presentation)
- No midterm or final

Homeworks

- Goals:
  - Learn to do critical reviews on privacy papers
  - Extract privacy requirements/concerns from text-based scenarios
  - Investigate tools for privacy risk mitigation
  - Review TED talks on privacy
- Individual assignments
- When submitting any report:
  - Use your own words when describing the papers or other material you find online
  - Do not borrow words from the authors (unless you are referring to a specific technical term, e.g., information disclosure)

Case Studies

- In class exercises
- Investigate privacy incidents
  - Work individually and in groups
  - Aggregate and analyze results
  - Present findings
- Play a privacy card game (if everything goes well . . .)
  - Play individually
  - Play in groups
  - Analyze strategies

Projects

- Goals:
  - Give you experience (both research and development) on a specific topic related to privacy
  - Collaboration within group members as well as among groups
  - Work with deadlines, prepare deliverables, present work done
- Work in groups of 2–3
- A project can be chosen by multiple groups
- Encourage publication from good projects

Research Interests

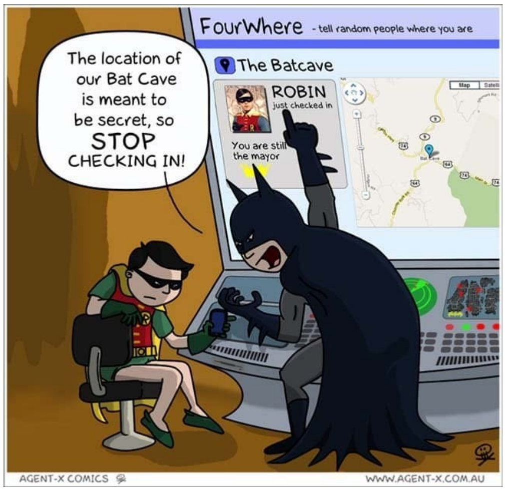
- Artificial intelligence
- Multiagent systems
- Computational logic
- Online social networks (OSN)
- Strategic games

Topics

- Web/Online Social Networks Privacy
- Artificial Intelligence for Privacy
- Usable Privacy
- Privacy Perceptions
- Misc Topics

Topics: Web/Online Social Networks Privacy

- Growing privacy concerns in online social networks
- Sharing behaviors of users
- Common violations and regret scenarios
- Methods for targeted advertising and how to mitigate those
- K-anonymity for ensuring privacy of datasets


FourWhere - tell random people where you are
The Batcave
ROBIN
just checked in
You are still the mayor
The location of our Bat Cave is meant to be secret, so STOP CHECKING IN!
AGENT-X COMICS
WWW.AGENT-X.COM.AU

Foursquare app: https://www.buzzfeed.com/ashleyperez/creepers-r-us

Topics: Artificial Intelligence for Privacy

- Privacy aware autonomous systems
- Design and maintenance of autonomous systems using AI techniques such as negotiation and argumentation
- Frameworks for elicitation, modeling, and verification of privacy requirements
- Privacy norms
- Privacy breaches as norm violations

Topics: Usable Privacy

- Designs for usable privacy interfaces
- Privacy nudges for warning users of potential privacy risks
- Semantic analysis of privacy policies

Topics: Privacy Perceptions

- Studies and surveys regarding human mental models about privacy concerns
- Differences among cultures
- Longitudinal studies about changes in privacy perceptions

Misc Topics

- Crowdsourcing privacy policies
- Mobile application privacy
- Privacy measurement

Learning Outcomes

- Learn various evaluation methods: Empirical, formal, case studies
- Understand personal identifiable information in databases and techniques to anonymize and protect such information
- Describe attacks against anonymized datasets
- Understand privacy risks when sharing personal data online and design mechanisms for mitigating such risks
- Describe privacy requirements and AI techniques for designing privacy-aware autonomous systems
- Design usable privacy interfaces and tools that balance privacy preserving and user functionality
- Identify and describe important elements of privacy policies and regulations
- Understand human attitudes to and perceptions of privacy

Outcomes (For the Instructor)

- Convert some of you into the world of academics
- Assignments prepared accordingly to give you research experience
- Even if you choose a developer path, you will be able to develop software with privacy awareness

Lectures

- Look at a common and important privacy problem
- Start with problem description
- Look at real world applications/cases and potential implications
- Learn about sample solutions
- Short exercises throughout
- Collaboratively analyze relevant incident(s) from the Privacy Incidents Database (Bring your laptop)
  1. Think individually
  2. Discuss with your neighbor
  3. Class discussion

Privacy

- Privacy is very important . . . whatever it is
- J. J. Thomson: “Perhaps the most striking thing about the right to privacy is that nobody seems to have any clear idea of what it is”
- A good or a bad thing? A right or a preference?

- Physical privacy:
  - “Right to be left alone”
  - “Freedom from unauthorized intrusion”
- Privacy is very broad
- Scope it to *data privacy*

Kieron O’Hara. The Seven Veils of Privacy. IEEE Internet Computing, 20(2):86–91, 2016

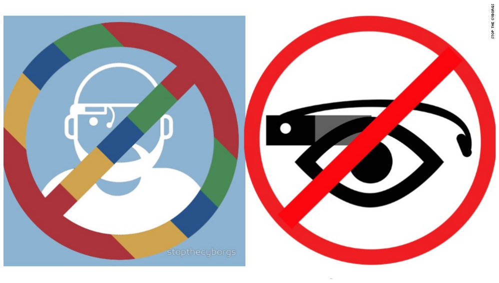
Oops, They Did It Again

- 13 hospital workers fired in LA for snooping in Britney Spears’ medical records
  - HIPAA prohibits accessing medical records without a valid reason
  - Violation: Just because she’s a celebrity is not a valid reason
- How to detect such violations?
  - Role-based access control
  - Log access
  - Are those enough?

http://www.avant.org.au/news/20160622-improper-access-of-medical-records/

http://articles.latimes.com/2008/mar/15/local/me-britney15

How the Camera Doomed Google Glass



- Early adopters
  - Usability: “It was not very useful for very much”
  - Privacy: “Disturb people around me that I have this thing”
- Mitigation: Use the same way we use sunglasses – usually taken off when we’re with people

http://www.cnn.com/2013/12/10/tech/mobile/negative-google-glass-reactions/index.html

https://www.theatlantic.com/technology/archive/2015/01/how-the-camera-doomed-google-glass/384570/

Target Discovers Pregnancy Before Parents

- Identify 25 products that indicate potential pregnancy, send coupons accordingly
- Dad goes to store to show coupons sent to her teenage daughter
- Mitigation: Mix in ads that pregnant women never buy, so baby ads look random

http://www.businessinsider.com/the-incredible-story-of-how-target-exposed-a-teen-girls-pregnancy-2012-2

Privacy Definitions

- Numerous examples
- Let’s try to come up with some definitions

Privacy Incidents

- An instance of accidental or unauthorized collection, use or exposure of sensitive information about an individual
- An event that creates the perception that unauthorized collection, use or exposure of sensitive information about an individual may happen

https://sites.google.com/site/privacyincidentsdatabase/

Data Collection, Storage, and Usage

- Collection: What personal information is collected by organizations?
- Storage: How do organizations store personal information? Is it kept secure?
- Usage: How do organizations use personal information? Whom do they share it with? Do they make users aware, e.g., ask for consent?

Contextual Integrity

- Ensuring appropriate information flows respectful of social norms in a given context
- Norm: Patient health information should not be disclosed
- Context:
  - During a consultation, it's appropriate for a patient to disclose health information to the doctor
  - Doctor may consult a colleague about the patient to exchange diagnosis
- How about doctor disclosing health information to a doctor friend at a party? Same action, different setting

Nissenbaum. Privacy in Context: Technology, Policy and the Integrity of Social Life. Stanford University Press, 2009

Normative Privacy

- Norms, expectations, conventions, regulations
- When a crime victim tells police about perpetrator, does it violate criminal's privacy?
- In this case, the norm works against privacy, for good social reasons

- Alice wants personal space
  - Puts a fence around her house
  - Few people cross it
  - Although there's nothing physical to stop them
- Patient consultation example: Alice expects confidentiality (her health information won't leave the medical system)

Kieron O'Hara. The Seven Veils of Privacy. IEEE Internet Computing, 20(2):86–91, 2016

Sociotechnical Systems

- People and software

- Technical and social considerations meet

- Interactions
  - User use software
  - Users interact with each other
  - Software components communicate with each other

Laws and Sanctions

- Norms can be turned into laws or regulations
- Not only conventional but also compulsory
- Sanctions would apply in case of violations
- Privacy law: Organizations' practice with personal data

Kieron O'Hara. The Seven Veils of Privacy. IEEE Internet Computing, 20(2):86–91, 2016

Privacy Engineering

- Integrating privacy solutions into everyday engineering practices
- Data protection requirements
- Beyond data breaches: Perceptions matter too

Seda Gürses and Jose M. del Alamo. Privacy Engineering: Shaping an Emerging Field of Research and Practice. IEEE Security & Privacy, 14(2):40–46, 2016

Transitional Privacy

- Privacy through friends
- Cannot always control what other people do

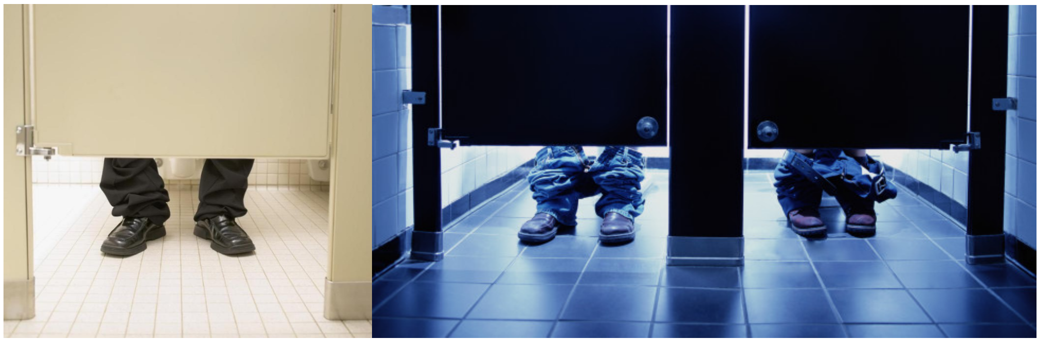
Typical Privacy Problems

- Identify common privacy problems
- Analyze sample solutions

Inference

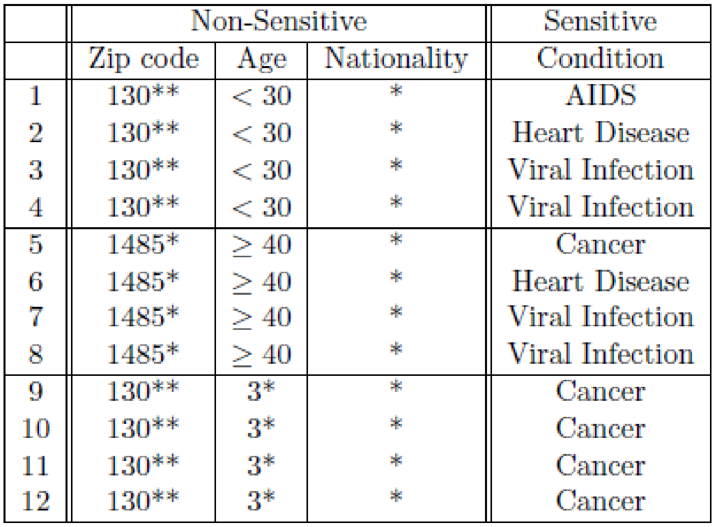
http://www.huffingtonpost.com/2013/11/13/smartphones-restrooms-bed-use-survey_n_4266701.html

Inference Possible



- The guy on the left is significantly different from the others
- When you see him outside (new information), you might recognize

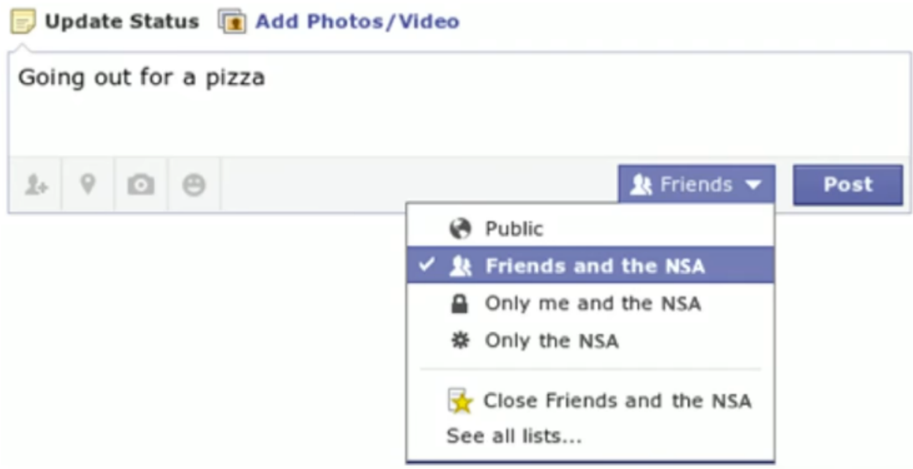
Anonymization of Datasets



	Non-Sensitive			Sensitive
	Zip code	Age	Nationality	Condition
1	130**	< 30	*	AIDS
2	130**	< 30	*	Heart Disease
3	130**	< 30	*	Viral Infection
4	130**	< 30	*	Viral Infection
5	1485*	≥ 40	*	Cancer
6	1485*	≥ 40	*	Heart Disease
7	1485*	≥ 40	*	Viral Infection
8	1485*	≥ 40	*	Viral Infection
9	130**	3*	*	Cancer
10	130**	3*	*	Cancer
11	130**	3*	*	Cancer
12	130**	3*	*	Cancer

- Provide researchers with useful data
- Protect user privacy by anonymizing columns and rows

Sharing Content



Update Status
Add Photos/Video

Going out for a pizza

Friends
Post

Public
✓ Friends and the NSA
Only me and the NSA
Only the NSA
Close Friends and the NSA
See all lists...

https://www.ted.com/talks/alessandro_acquisti_why_privacy_matters#t-53301

Unintended Disclosure

- Intrusion, embarrassment
- Unintended audience

http://www.cbsnews.com/news/senator-pat-roberts-unexpected-ringtone-frozen-let-it-go/

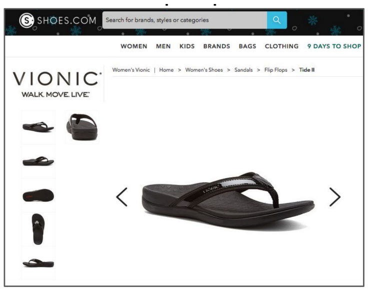
Sharing vs Revealing

- To whom your shared content will reach
- “If I cannot shout it out in the middle of downtown, I’d not say it online”
- Differential privacy: You may share, but not reveal anything

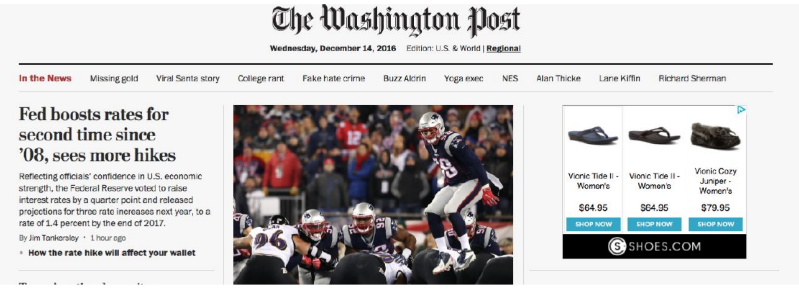
Regrets

- Regrettable actions, e.g., send email to wrong recipients
- How to avoid those

Targeted Advertising


SHOES.COM
Search for brands, styles or categories
WOMEN MEN KIDS BRANDS BAGS CLOTHING 9 DAYS TO SHOP
VIONIC
WALK. MOVE. LIVE.
Women's Vionic | Home > Women's Shoes > Sandals > Flip Flops > Tide II

Look at shoes at store


The Washington Post
Wednesday, December 14, 2016 Edition: U.S. & World | Regional
In the News Missing gold Viral Santa story College rant Fake hate crime Buzz Aldrin Yoga exec NES Alan Thicke Lane Kiffin Richard Sherman
Vionic Tide II - Women's $64.95 SHOP NOW
Vionic Tide II - Women's $64.95 SHOP NOW
Vionic Cozy Juniper - Women's $79.95 SHOP NOW
SHOES.COM

Fed boosts rates for second time since '08, sees more hikes

Reflecting officials' confidence in U.S. economic strength, the Federal Reserve voted to raise interest rates by a quarter point and released projections for three rate increases next year, to a rate of 1.4 percent by the end of 2017.

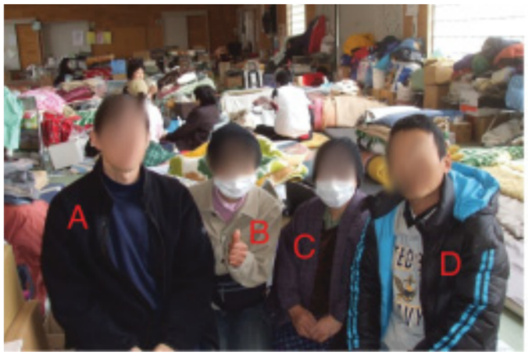
By Jim Tankersley · 1 hour ago

- How the rate hike will affect your wallet

They come with you to the news

- How does it happen?
- How can you avoid it?

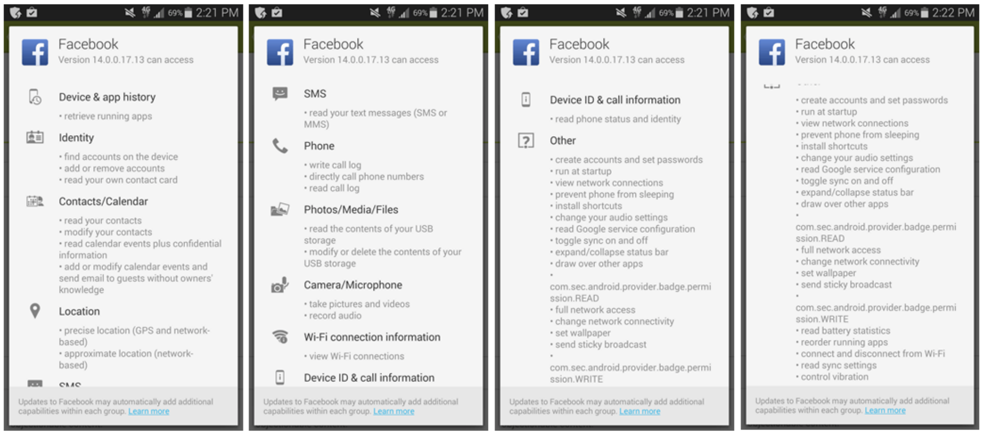
Multiparty Privacy: Argumentation



- After tsunami disaster
- Arguments for/against sharing the picture
  - Not share: Hand gestures not appropriate
  - Share: Shows difficult situation of survivors, would encourage people to help

Fogués et al. Sharing Policies in Multiuser Privacy Scenarios: Incorporating Context, Preferences, and Arguments in Decision Making. ACM Transactions on Computer-Human Interaction, 24(1):5:1-5:29, 2017

AI for Privacy: Negotiation



Facebook
Version 14.0.0.17.13 can access

Device & app history
• retrieve running apps

Identity
• find accounts on the device
• add or remove accounts
• read your own contact card

Contacts/Calendar
• read your contacts
• modify your contacts
• read calendar events plus confidential information
• add or modify calendar events and send email to guests without owners' knowledge

Location
• precise location (GPS and network-based)
• approximate location (network-based)

SMS

Updates to Facebook may automatically add additional capabilities within each group. Learn more

Facebook
Version 14.0.0.17.13 can access

SMS
• read your text messages (SMS or MMS)

Phone
• write call log
• directly call phone numbers
• read call log

Photos/Media/Files
• read the contents of your USB storage
• modify or delete the contents of your USB storage

Camera/Microphone
• take pictures and videos
• record audio

Wi-Fi connection information
• view Wi-Fi connections

Device ID & call information

Updates to Facebook may automatically add additional capabilities within each group. Learn more

Facebook
Version 14.0.0.17.13 can access

Device ID & call information
• read phone status and identity

Other
• create accounts and set passwords
• run at startup
• view network connections
• prevent phone from sleeping
• install shortcuts
• change your audio settings
• read Google service configuration
• toggle sync on and off
• expand/collapse status bar
• draw over other apps
• com.sec.android.provider.badge.permission.READ
• full network access
• change network connectivity
• set wallpaper
• send sticky broadcast
• com.sec.android.provider.badge.permission.WRITE

Updates to Facebook may automatically add additional capabilities within each group. Learn more

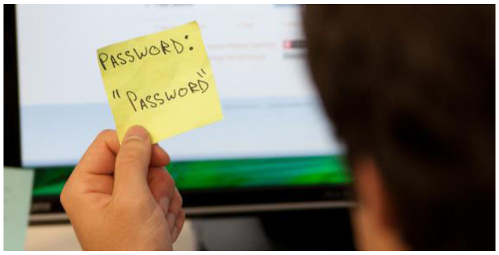
Facebook
Version 14.0.0.17.13 can access

• create accounts and set passwords
• run at startup
• view network connections
• prevent phone from sleeping
• install shortcuts
• change your audio settings
• read Google service configuration
• toggle sync on and off
• expand/collapse status bar
• draw over other apps
• com.sec.android.provider.badge.permission.READ
• full network access
• change network connectivity
• set wallpaper
• send sticky broadcast
• com.sec.android.provider.badge.permission.WRITE
• read battery statistics
• reorder running apps
• connect and disconnect from Wi-Fi
• read sync settings
• control vibration

Updates to Facebook may automatically add additional capabilities within each group. Learn more

- Runtime configuration of app permissions
- Negotiation between the user and the app provider

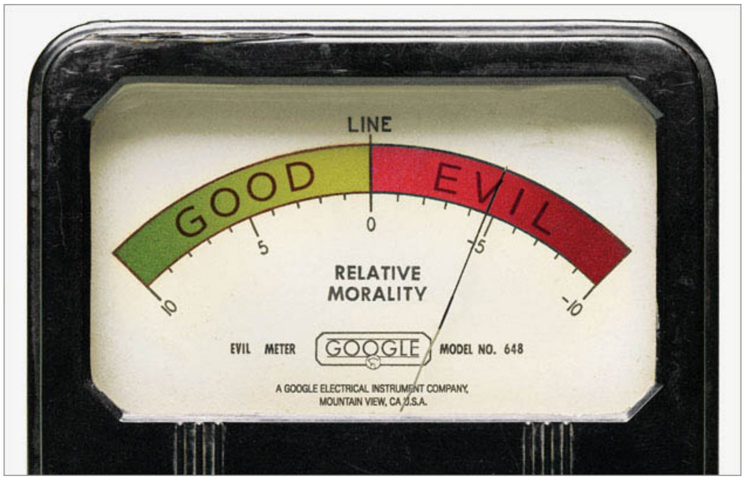
Usable Privacy



- Utility vs privacy: You want my password or a dead patient?
- How to prevent privacy messing up functionality?

Koppel et al. Workarounds to computer access in healthcare organizations: You want my password or a dead patient? Studies in Health Technology and Informatics, 208:215220, 2015

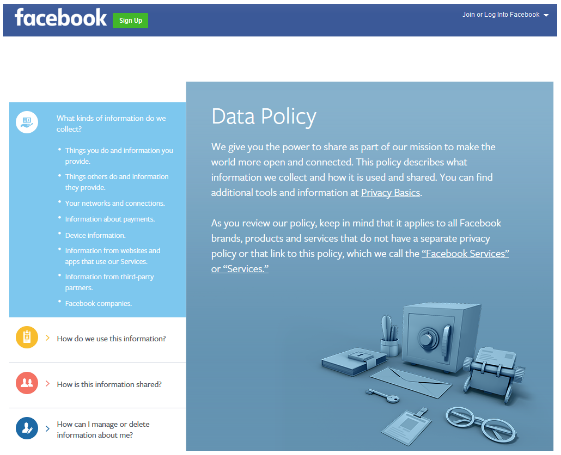
Metrics and Measurement



- How much privacy is enough? Or too much?

https://pusz4frog.wordpress.com/category/technology-2/

Privacy Policies



What kinds of information do we collect?

- Things you do and information you provide.
- Things others do and information they provide.
- Your networks and connections.
- Information about payments.
- Device information.
- Information from websites and apps that use our Services.
- Information from third-party partners.
- Facebook companies.

How do we use this information?

How is this information shared?

How can I manage or delete information about me?

Data Policy

We give you the power to share as part of our mission to make the world more open and connected. This policy describes what information we collect and how it is used and shared. You can find additional tools and information at Privacy Basics.

As you review our policy, keep in mind that it applies to all Facebook brands, products and services that do not have a separate privacy policy or that link to this policy, which we call the "Facebook Services" or "Services."

- Nobody reads privacy policies
- Facebook privacy policy is longer than the US constitution

http://www.huffingtonpost.com/2010/05/12/facebook-privacy-policy-s_n_574389.html

Westin Privacy Index

- Classify the public into three categories
- Fundamentalist (25% of Americans): Distrustful of organizations, refuses to give out personal information
- Pragmatist (55% of Americans): Weighs the value of consumer opportunities, aware of privacy risks
- Unconcerned (20% of Americans): Doesn't know what the "privacy fuss" is about

Westin. Privacy and Freedom. Administrative Law Review, 22(1):101–106, 1969

Privacy Surveys

- Why are user studies on privacy not convincing?
- Question: How would you feel about a mobile app that tracks your location whereever you go? [You cannot turn it off]
- How about: The app offers discount coupons based on your favorite locations
- How about: The app sends your location to third parties . . . potentially malicious people might access your location
- Incentives change based on circumstances
- Privacy paradox: Reported vs actual behavior

Cultural Differences

Not so private

More private

Wisdom of Crowd